Design and Implementation of Integrated Encrypted EMAIL for Clinicians

Peter Tarczy-Hornoch, M.D., Harold I. Goldberg, M.D., Sherrilynne Fuller, Ph.D.
IAIMS Program, University of Washington, Seattle, WA

INTRODUCTION

Access to both patient specific information as well as information about the domain of medicine is critical to clinical care. As part of the University of Washington IAIMS effort we are developing tools to provide easy access to both types of information at the point of care. Encrypted EMAIL is one such tool.

EMAIL is inappropriate for sensitive clinical material. It has been likened to a postcard in that the contents can relatively easily be read en route[1]. It can be inadvertently misdelivered to an unintended recipient. Finally there are significant unresolved questions regarding the medicolegal implications of clinically related EMAIL communications including discoverability[2]. Despite these concerns, clinicians use medical listservers to share information about the practice of medicine[3]. Preliminary results from a survey of two such list servers show clinicians use EMAIL for work related purposes 4.1 hours/week (SD=2.9, n=2338, 33% respondents)[4].

A collaborative research project led by IAIMS was undertaken to provide PGP[1] encrypted EMAIL to clinicians at the University of Washington.

METHODS

Computing and Communications (C&C) developed extensions for PGP[1] encryption (Ver 2.6.2) within the campus PINE EMAIL package. These include: encryption as a simple filter, a transparent (to the end user) public key ring, requiring the pass phrase to be entered only once/session, and creating utilities to create PGP keys and manage the keyring.

IAIMS personnel (n=4), C&C (n=2) and a limited number of clinicians (n=5) participated in a six month alpha design and test phase to make encryption/decryption as transparent and easy to use as possible within the campus EMAIL framework.

Medical Center Information Systems (MCIS) and IAIMS personnel attempted to extend the testing to a beta group of ~100 specialist and generalist clinicians in inpatient and outpatient settings. The goals of the beta phase were to: 1) confirm the scaleability of PGP encryption, 2) further refine the user interface, 3) identify areas of high added value for automated encrypted clinical alerts, 4) identify any other issues.

RESULTS

The design and alpha implementation of integrated PGP encryption was successfully completed. The alpha testing resolved a number of issues: 1) the need for further streamlining of invocation of encryption, 2) addition of a medical spell checker to PINE, 3) preliminary identification of areas for automated encrypted clinical alerts. The beta testing revealed 1) problems with scaleability of PGP to a large group of users, 2) the need to accommodate installed divisional EMAIL packages (non-PINE), 3) evolution of industry standards away from PGP toward S/MIME

DISCUSSION

The collaboration between IAIMS, C&C, and MCIS as well as the support of the University of Washington Hospital Medical Directors have been key to the accomplishments thus far. The recognition amongst clinicians of the need for encryption is encouraging. Optimal targets for encrypted clinical alerts have yet to be finalized. We have, however, identified the characteristics of the types of information that should receive priority for inclusion in automated encrypted EMAIL alerts. The information should be time sensitive, clinically important, potentially sensitive, and hard to obtain via other routes.

CONCLUSION

Clinicians see the need for encrypted EMAIL, particularly automated clinical alerts. PGP does not appear a viable solution due to problems of scaleability and industry trends toward alternate forms of encryption. Ultimate success at integrating encrypted EMAIL into clinical practice at the University of Washington appears likely especially with adoption of industry standards (S/MIME).

ACKNOWLEDGMENTS

Supported in part by an NLM IAIMS Implementation Grant. Additionally invaluable computing and personnel resources were donated by C&C, MCIS and the alpha and beta testers.

REFERENCES

1. Garfinkel S. PGP: Pretty Good Privacy. O'Reilly and Associates Inc. 1995.
2. Elliott SJ, Elliott, RG. Internet List Servers and Pediatrics: Newly Emerging Legal and Clinical Practice Issues. Pediatrics, 1996; 97:399-400
3. Tarczy-Hornoch P. NICU-Net: An Electronic Forum for Neonatology. Pediatrics, 1996; 97:398-9
4. Weigle, GM, Zollo, MB, Tarczy-Hornoch, P, Effects of international EMAIL discussion groups on clinical practice in pediatric and neonatal intensive care, Int Care Med, 1996; 22:S199